non-expert persons tasked with preserving digital forensic evidence, the cumbersome process of accessing the guidelines via paper media increases the risk of mistakes. Furthermore, since the work procedures are included in itemized statements, the flow of work in relation to the passage of time is often unclear.

With these issues in mind, we developed our Guideline Total Support System (GSS) in order to support work based on the Guidelines for Preservation of Evidence. GSS is a program that runs on personal computers (PCs) and Android operating system (OS) terminals, such as tablets and smartphones. An advantage of using an Android terminal is that it supports various user interfaces, and thus allows first responders to work step by step.

The complete system consists of three components: the first supports the creation of contents for display on an Android terminal from paper guidelines, the second is the guideline execution section for first responders, and the third is a function that allows the system to generate an output report based on the first two components. In this paper, the authors report on improvements to the first and second components, and the development of the third. Additionally, after applying the complete system to a small trial scenario based on an actual incident, an evaluation on the utility and effectiveness of the system was conducted.

In the sections below, we present an overview of the GSS and the results of an evaluation in which the developed system was applied to a simulated incident. Although there have been numerous previous papers dealing with digital forensics, such as Refs. [4], [5], [6], the authors have not been able to identify any works that deal with a guideline support system for digital forensics other than their own.

## 2 PRESERVATION OF EVIDENCE AND RELATED GUIDELINES

### 2.1 Preservation of Electromagnetic Evidence

The preservation of electromagnetic evidence involves the retention of digital data related to incidents, dishonest acts, or crimes. According to the Guidelines for Preservation of Evidence, the most important duty of the digital forensics operator is collecting, acquiring, and preserving as much data as possible. If this procedure is defective, doubts may arise regarding the validity of the original evidence. Therefore, this work is extremely sensitive.

### 2.2 Guidelines for Preservation of Evidence

The abovementioned Guidelines for Preservation of Evidence set digital forensics standards related to the preservation of electromagnetic evidence in Japan. These guidelines are intended for use by first responders, including non-experts. The third edition, published in 2013, comprises 67 pages in five chapters and appendices. An overview of the contents is provided below:

Chapter 1: Preparations to perform beforehand

- This chapter describes procedures to be taken and tasks to be performed before an operator engages in evidence preservation work.

Chapter 2: Response after an incident is discovered

- This chapter describes urgent work that should be performed after an incident occurs, such as getting a grasp of the overall situation.

Chapter 3: Collection, acquisition, and maintenance of physical objects

- In this chapter, the types of objects and the work procedures, which will depend on the situation at an incident, are explained to the operator.

Chapter 4: Preparation of devices required to maintain evidence

- In this chapter, the equipment needed to preserve evidence is explained.

Chapter 5: Evidence preservation during and after acquisition

- In this chapter, contents that an operator should preserve during and after acquisition work is explained.

## 3 DEFINITION OF SYSTEM REQUIREMENTS

We explored the questions, "What kind of person should be supported in evidence prevention work?" and "What kind of system should be realized?" From some investigations, we defined the intended users of our system as persons belonging to educational institutions or private companies that do not possess deep knowledge regarding digital forensics [7] [8] [9]. On the other hand, we found that 45.1% of the company employees surveyed used Android OS-equipped smartphones for business [10]. Therefore, because we thought it would be effective to base our system's incident-related correspondence on the portable terminals that are carried by operators under normal circumstances, the Android OS was adopted as the base for our application.

Next, it was necessary to determine which functions the system would be tasked with performing. We performed this definition requirement in cooperation with the technical subcommittee workgroup of the Institute of Digital Forensics. Together, we concluded that it would be necessary to meet the following requirements:

1. Creation of an Android-based guideline file from the paper guidelines.
2. Implementation of structured procedure-based work guides that could be accessed via an Android terminal.
3. Recording and verifying information that assures the integrity of the work performed
4. Ensuring various interfaces supported by the Android terminal also support the application.
5. Outputting reports about the done work

Although the Android-based smartphone application was capable of supporting the second, third, and fourth requirements described above, meeting the first and fifth requirements necessitated the use of a PC. Therefore, we decided to develop a tool that would operate in conjunction with a PC to create the guideline file and output the final report. This meant that an integrated Android and PC system would be developed and applied.

## 4 GUIDELINE TOTAL SUPPORT SYSTEM

Our system was named the Guideline Total Support System (GSS) based on our hope that it will be applicable to future information security guidelines in addition to the previously mentioned Guidelines for Preservation of Evidence. The GSS consists of three programs based on the requirements defined in Section 3. Our previous efforts related to GSS development are described in Refs. [11], [12]. An overview of the system is shown in Fig. 1, and an outline of each program is shown in Table 1.

The program that hosts the guideline on the Android terminal is known as the "GSS-Executor," while the "GSS-Creator" is the program that creates and edits the guide read by the GSS-Executor. For the latest version, the

executable guidelines file was replaced by updating the GSS-Executor.

In this version, the first responder reads guideline data onto his or her own Android terminal. After the preservation work, other persons involved in the incident response can then check records related to the work performed via the report output program named "GSS-Reporter."

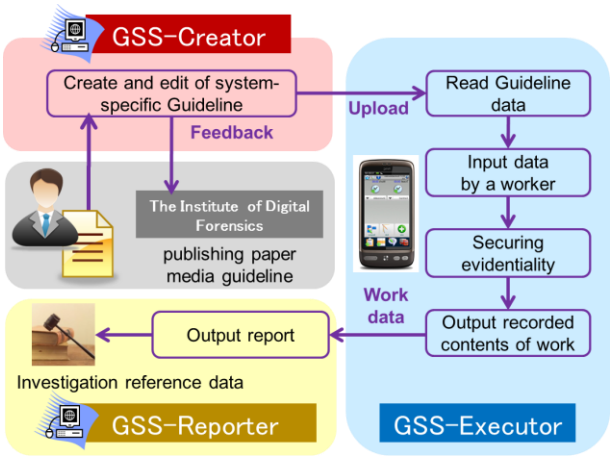


**Figure 1:** Overview of the Guideline Total Support System (GSS)

**Table 1**: Application program overview

| Program name | Outline |
|---|---|
| **GSS-Creator** | ● Create and edit guideline for GSS-Executor<br>● Upload guideline to server |
| **GSS-Executor** | ● Android application<br>● Acquire guideline data from server<br>● Execute guideline and input information |
| **GSS-Reporter** | ● Output work report |

We developed our system based on the premise that the widespread use of the Android OS on various mobile devices would facilitate the rapid creation of situation specific guidelines. Accordingly, a detailed Android interface was set up for every guideline item generated by the GSS-Creator. These interfaces are explained in Section 5.3.

## 5 GSS-CREATOR

### 5.1 Guideline Creation Program and Issues

To create a guide on an Android terminal, it was first necessary to systematize the guideline information, develop the GSS-Creator program on a PC, and then create and edit the Android terminal guideline. The GSS-Creator development environment is shown in Table 2.

**Table 2:** GSS-Creator development environment

| | |
|---|---|
| Development OSs | Microsoft Windows Vista Business, Microsoft Windows 8 Enterprise |
| Platform | Microsoft Visual Studio 2010 .NET Framework Version 4.0.30319 RTMRel |
| Language | C# |

During the process of defining the GSS-Creator development requirements, it was necessary to resolve the following issues:

1. How should the guideline be built?
2. What kind of data structure is most suitable for the guideline?
3. What is the best way to modify a guideline edited for paper media into system-oriented data?
4. How can we determine whether the created guideline is correct?

Regarding the first point, it was important to create a simple, visually intelligible operating environment. Therefore, to express work procedures in a time series, our proposed guideline building method uses flowcharts and blocks. This method will be explained in more detail in the next section.

As for the second point, we were unsure as to the type of data structure that should be handled in this system because work contents in the Guidelines for Preservation of Evidence are classified by onsite situations (see Table 3). This makes it difficult to define single-flow start-to-finish work procedures. Our solution was to make Extensible Markup Language

(XML) format files in GSS-Creator in order to classify the work in onsite situations. Since XML is used for describing the meaning and structure of data, it was felt that its layered structure could appropriately express conditional branches in the guidelines. Furthermore, since the XML format allows multiple attributes for single information, different behaviors can be defined on Android terminals depending on the work contents.

**Table 3.** Response to an incident (from Chapter 2 of the Guidelines for Preservation of Evidence)

| |
|---|
| 2.2.3 Case countermeasures if Coping is insufficient<br>● When an information shortage is checked, conduct interviews or gather information to fill in blank spots<br>● When excessive information has been gathered, apply standards and reason to the collected information, and when you determine a piece of information is unnecessary, delete it. |

Regarding the third and fourth points, we experienced misgivings about potential deviations arising between GSS and paper media guidelines. This problem is rooted in the policies adopted make the guideline more suitable for the GSS system. Normally, when a problem arises in the existing guideline, the system takes into consideration feedback to the workgroup. To that end, it was considered necessary to share any changes to the flowchart that had been applied to the paper media guideline.

In response, we decided to use the Cacoo Web-based application, which provides diagram creating and sharing services [13], to handle the flowcharts. This allows the GSS to collect opinions about the contents and order of the blocks and flowcharts from system users and officials. Figure 2 shows the "Cacoo" flowchart-sharing screen.

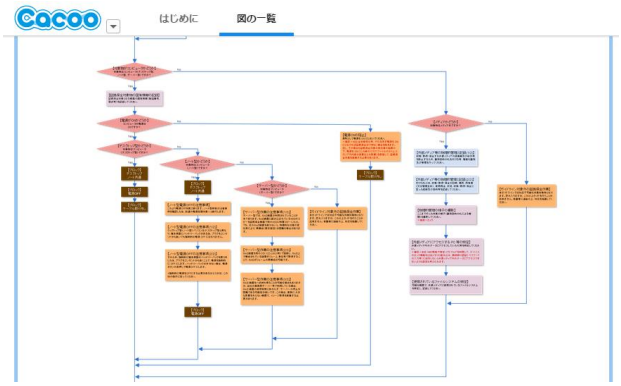


**Figure 2:** Cacoo flowchart sharing screen

### 5.2 Expression Using Flowcharts and Blocks

In our system, flowcharts are used to express process flows. This allows a series of procedures to be expressed intelligibly from start to finish, and the junctions that occur after conditional branches to be expressed easily. In digital forensics research, flowcharts are used for systematization of the work procedures used to preserve evidence in mobile forensics [14]. However, the objective is only to express the forensic guide as a flowchart, and the result is not used for realization of a program. In this research, we use flowcharts to express the process flows specified by the guidelines in our program.

When printed, the Guidelines for Preservation of Evidence consists of approximately 60 pages of A4 paper. However, if we were to include that much information in one flowchart, it would be difficult for an operator to grasp all aspects of the guideline. Therefore, in this study, we defined blocks for storing flowchart data. This allows improved visibility and usability to be achieved at the time of guideline creation. Such blocks are used as a programming subroutine. An illustration of a flowchart and an associated block is shown in Fig. 3.

ISBN: 978-1-941968-01-7 ©2014 SDIWC

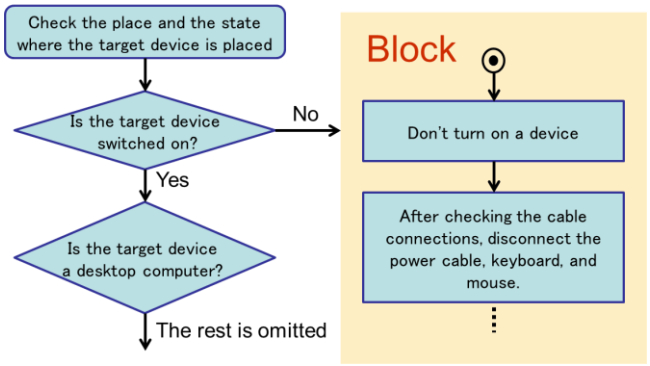


**Figure 3:** Image of flowchart and block

## 5.3 Types of Work

The Guidelines for Preservation of Evidence requires the operator or first responder to perform various types of work when an incident occurs. However, the results of survey analysis on work items revealed that, in GSS-Creator, work items could be classified into five types (see Table 4).

**Table 4**: GSS-Creator Work items

| Item name | Work item contents |
|---|---|
| **Note item** | Issues cautions to an operator |
| **Select item** | Requires an operator to choose from two or more items |
| **Processing item** | Requires processing by an operator |
| **Record item** | Requires recording of the situation at the scene by an operator |
| **Branch** | Depending on the contents of the selection, branch occurs |

## 5.4 Function of GSS-Creator

Figure 4 shows the main screen of the GSS-Creator. On the right-hand side of the application screen, a flowchart is used to create a guideline. On the left-hand side of the application screen, the list of blocks that exist in a guideline and the flowchart overview are displayed. By choosing an action from a menu, the flowchart block displayed on a screen can be changed.

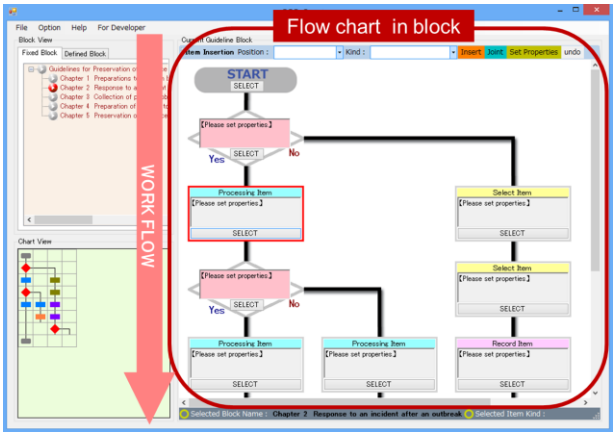


**Figure 4**: GSS-Creator guideline creation screen

Guideline creation is performed by arranging a work item and a conditional branch item in a flowchart. When an item is inserted in a flowchart, it is necessary to set its properties. Under a selection item, it is possible to set a selection method and the number of contents, along with an actual content other than a common input property. For a recording item, it is necessary to set an input interface that can be called on an Android terminal. The contents that can be set are shown in Table 5. Since Android terminals allow the input interface that is called at the time of guideline creation to be set, the operator can choose from among several different interfaces.

**Table 5**: Details of settable input interfaces

| Interfaces | Available Android terminal functions |
|---|---|
| **Text box** | A software keyboard is shown where you can input characters |
| **Time selection** | The interface that chooses a date and time can be used |
| **Numerical input** | The function that chooses a numerical value by a swiping operation on the screen can be used |
| **Voice recording** | The Android media recorder function can be called and sound recording can be performed |
| **Camera** | The Android camera function can be called and video or photo recording of the scene can be taken. |

ISBN: 978-1-941968-01-7 ©2014 SDIWC

## 6 GSS-EXECUTOR

### 6.1 Guideline Execution Tool

The guideline file created by GSS-Creator is distributed with the Android GSS-Executor application. In GSS-Executor, the guideline created by GSS-Creator can be followed reliably using the flowchart. The GSS-Executor development environment is shown in Table 6.

**Table 6**: GSS-Executor development environment

| | |
|---|---|
| Development OS | Microsoft Windows 8 Enterprise |
| Integrated development environment | Eclipse 4.2 Juno |
| SDK | Android SDK 4.1 |
| Language | Java 1.6.0_43 |

### 6.2 GSS-Executor Function

The XML format guideline created by GSS-Creator can be executed by GSS-Executor on an Android terminal. GSS-Executor reads information for every tag that stores work contents and attributes in the XML guideline executable file, and then displays the contents on the terminal screen as appropriate. Execution screens for a GSS-Executor guide are shown in Fig. 5. A button displaying the work title, type of work, and a note dialog box is located in the upper section of the application screen. Buttons for changing to the next task are located in the lower section of the screen. Depending on the work item type, the input-output interface is updated dynamically and arranged in the central portion of the screen.
The central screen changes according to the flowchart and blocks defined in GSS-Creator. On a conditional branch item screen, the next item of work changes from "Yes" or "No" depending on the worker's choice. Since this movement is defined by the flowchart, the worker can perform quick processing specific to the situation at the scene.


**Figure 5**: GSS-Executor execution screens

The screen on the left-hand side of Fig. 5 shows a selection example. In this example, for the contents "choose the incident generation detection circumstances," two or more items can be selected and recorded by checking the appropriate boxes. The screen on the right-hand side of Fig. 5 is captured by the camera function, with which the first responder can photograph the initial condition of a preservation subject.
Multiple sheet photographs can be taken and memos can be attached to each photograph. The voice recording function provides another record keeping tool with which the first responder can orally describe the situation and record any unusual sounds being emitted by the equipment. It is also possible to conduct a check after recording.

### 6.3 Function for Securing Evidentiality

In this version, we have implemented the following three functions to improve the quality and accuracy of GSS-Executor generated data:

(1) Justifying the error of time used in the Android device
(2) Obtaining Android device position information using the Global Positioning System (GPS) function
(3) Isolating equipment from network

ISBN: 978-1-941968-01-7 ©2014 SDIWC

These functions are used at the starting point of the forensic work. If the work is interrupted, the system prompts the operator to use these functions again when it is restarted.

### 6.3.1 Confirmation of the Error of the Terminal Time

GSS-Executor records the time at which the work was performed. However, in such cases, it is possible that an error between the correct time and Android device time will exist. To eliminate such errors, we implemented a mechanism that checks for system clock errors and the correct time using Network Time Protocol (NTP), which is a communication protocol for synchronizing equipment to the correct clock time. In Android, since the Apache Commons Net provides an NTP connection library, we used it to produce the error confirmation function. The NTP time synchronization setting screen is shown in Fig. 6. The system also records time synchronization information into the terminal database.

### 6.3.2 GPS Function Position Information

To acquire accurate position information at the actual scene, which is important in evidence preservation work, we used the GPS function of the Android terminal. Although GPS is mainly used outdoors, we noted that there is a setting that can capture and record GPS satellite signals in the change of weather conditions or if you do the work at the window. When enabled by the operator before beginning work, the terminal's GPS function continues searching for GPS signals while the guideline is being worked. If GPS signals are captured, the system records the longitude and latitude of the scene into the database. Although, as described in the following section, the application will isolate the terminal's communication state when in the working state, no problem results because the GPS function operates independently of network connections.

### 6.3.3 Communication isolation

According to Computer Forensic Examiner – Quick Reference Guide published by The International Association of Computer Investigative Specialists, if the subject requiring preservation is connected to the network, it is normally necessary for the first responder to isolate the machine by disconnecting it from the network [15]. This is because it is possible that the machine state will change if the device remains connected to an external network.
Similarly, since the preservation target may be capable of performing wireless communications, GSS-Executor sets the Android device into Airplane Mode, thus cutting off both Wi-Fi and 3G network connections, isolating the Android terminal communication state, and thereby minimizing any effects on the machine being preserved. Furthermore, since an operator can intentionally make Wi-Fi connections even if the terminal is in Airplane Mode, the application monitors both the Wi-Fi and Airplane Mode states at all times when in the working state in order to record that information into the database.


**Figure 6:** NTP server connection screen

## 7 GSS-REPORTER

### 7.1 Extraction of Work Performance Information

The incident report is produced by the GSS-Reporter function, which works by reading the comma separator values (CSV) format work information file output by GSS-Executor. GSS-Reporter can also use a list display to check the information input by GSS-Executor and, when necessary, narrow down the type of information to be displayed. Since it is the same as that of GSS-Creator, the development environment for GSS-Reporter is omitted from this report.
Examples of items that can be extracted and displayed are shown in Table 7. If the work was not correctly performed due to erroneous terminal settings, or if there has been an attempt to perpetrate deliberate fraud in the work process, it will be possible to confirm the correct status from this screen.

**Table 7:** Item details that can be extracted

| Item name | Contents of the item |
|---|---|
| **Incident id** | Number given according to the incident |
| **Guide id** | Number given according to the guideline |
| **Sequence id** | Serial number of work |
| **Date and Time** | Date and time on which work was done |
| **Time accuracy** | Whether the time synchronization by NTP server connection was performed (see Section 6.3.1) |
| **GPS longitude** | The longitude information obtained from GPS |
| **GPS latitude** | The latitude information obtained from GPS |
| **Isolation** | Whether both 3G circuit and Wi-Fi were cut out |
| **Title** | The title of work |
| **Input** | Input contents (text, voice, and image) |
| **Is skip** | Whether work was skipped |
| **Tag** | The tag registered at the time of work |

### 7.2 Work Report File Output

GSS-Reporter can output entire or customized work report files because the application only outputs the items that have been selected in the check box. Thus, report output can be tailored to the demands of the partner's forensic team or operator. Since the work report is output in a file in HyperText Markup Language (HTML) format, its contents can be viewed using an Internet browser. Figure 7 shows a sample of a report file output by GSS-Reporter.

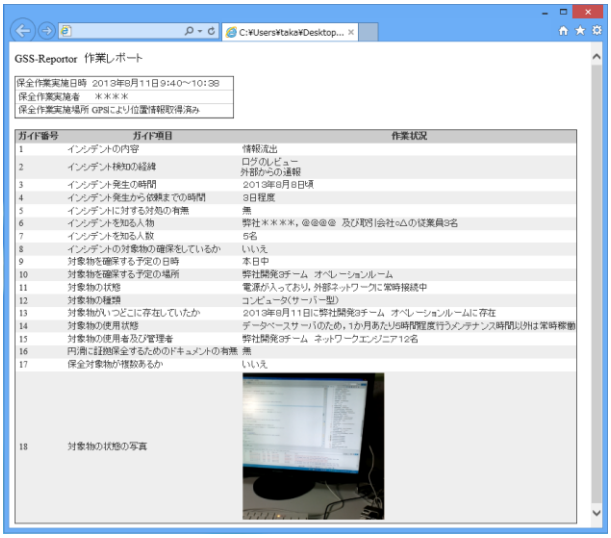


**Figure 7:** Work report output in HTML format

## 8 GSS-EXECUTOR AND GSS-REPORTER TRIAL APPLICATIONS

In order to determine whether the developed system is effective in an incident response situation, application experiments using a simulation scenario were performed. We began by examining the electromagnetic records of an incident that had actually occurred, after which the incident was used as the basis of our simulation scenario. The evaluation experiments were performed from the following two viewpoints: Viewpoint 1 is an evaluation of the overall utility of GSS-Executor and GSS-Reporter, while Viewpoint 2 is an evaluation of GSS-Executor and GSS-Reporter when compared with the paper media guideline.

### 8.1 Selection of the Simulation Subject

As mentioned above, an appropriate scenario simulation was written based on the organization incident response discussed in Section 2. According to an announcement by Japan Network Security Association (JNSA) in 2013, mismanagement was the most dominant cause of information leakage (38.9%) [16]. Therefore, information leakage was selected as the simulation subject for our evaluation.
The experiment was conducted with the assistance of 10 students of Tokyo Denki University. The information on the incident used for the scenario, which involved an educational institution, was published by the Information Security Forum NPO [17]. The simulation scenario based on this example is shown in Table 8.

**Table 8**: Simulation scenario

| |
|---|
| At the XYZ Laboratory of ABC University, researchers borrowed confidential information data from their business partner based on the understanding that the data were for research purposes only. A contract was executed between XYZ Laboratory and the company that stipulated that the laboratory must not, in any way, move the company data from the dedicated HDD containing the data, and that the HDD would be kept isolated from the laboratory network while it was in use. However, during the loan period, which spanned an extended period of time, persons concerned failed to strictly abide by the contract provisions and the confidential information was moved into a shared folder on a PC connected to the external network. When the problem is discovered, the faculty advisor who learned about the situation contacts the contracted company regarding the [test subject] and instructs the [test subject] to confirm immediately whether confidential information data have been accessed from outside the laboratory. When the [test subject] investigates the communication log, unauthorized access to the data concerned from outside is confirmed. The [test subject] decides to immediately carry out evidence preservation based on the present situation. |

After the above scenario was explained to the test subjects, Evaluations 1 and 2 were performed. In Evaluation 1, the test subjects were instructed to complete a series of jobs beginning at the start of evidence preservation using GSS-Executor and continuing through to outputting a work report using GSS-Reporter.

In Evaluation 2, the test subjects completed the same work using the paper media guidelines. We then examined any resulting differences that were noted between using the GSS and the paper media guidelines. In order to accomplish this, the test subjects were divided into two groups of five persons, and each group received separate execution orders to prevent test subject prejudices from impacting the evaluation results.

### 8.2 Application Evaluation 1

Evaluation 1 examined the functions of the system during actual GSS work. After the scenario shown in Table 8 was explained to the test subjects, evidence preservation was performed in accordance with the procedure memo outlining the experiment. The evaluation process, which was conducted after each test subject finished all the procedures, consisted of question items rated on a five-point scale. Common evaluation criteria and results are shown in Table 9.

**Table 9:** Common questions and evaluation

| | Questions | Average (n=10) |
|---|---|---|
| 1 | Do you think the experiment scenario was suitable? | 4.4 |
| 2 | Do you think that the information contained in the procedure memo was suitable for this experiment? | 3.7 |
| 3 | Do you think that, on the whole, the program was easy to operate? | 4.2 |

Table 9 results allowed us to determine whether the environment prepared for the experiment was suitable, and to evaluate the ease of use for the entire system. Next, the results of the GSS-Executor Android application evaluation are shown in Table 10.

**Table 10:** Questions and GSS-Executor evaluation results (n=10)

| | Questions | Average (n=10) |
|---|---|---|
| 1 | Do you think you would be able to use this program intuitively, even if not given an explanation? | 3.6 |
| 2 | Do you think the layout of each function is suitable? | 3.6 |
| 3 | Do you think the classification-by-color display of work is intelligible? | 4.5 |
| 4 | Do you think the tag registration function is suitable? | 3.6 |
| 5 | Did you think the display function of the relevant information is good? | 4.1 |
| 6 | Although preservation-of-evidence work requires speed and accuracy, do you think you could follow the guideline instructions quickly and correctly using this program? | 4.2 |

As can be seen in Table 10, these result allowed us to conclude that each interface was arranged in positions suitable for small terminals. However, a low score was obtained for Question 1, which asked whether the program could be used intuitively. From this, we have concluded that improvements are required for GSS-Executor. Finally, the evaluation results for the GSS-Reporter report output tool is shown in Table 11.

**Table 11:** Questions and evaluation results for GSS-Reporter (n=10)

| | Questions | Average (n=10) |
|---|---|---|
| 1 | Do you think you would be able to use this program intuitively, even if no explanation was provided? | 4.0 |
| 2 | Do you think the table output is suitable? | 4.7 |
| 3 | Do you think the manner in which item details can be extracted is suitable? | 4.7 |
| 4 | Do you think the report output function is useful? | 4.8 |

From these evaluation results, we have concluded that it will be necessary to implement a function that is capable of extracting selected data under more refined conditions, and that there is also a need to also consider the visibility of the outputted report.

## 8.3 Application Evaluation 2

In Evaluation 2, differences between using the GSS and the paper media guideline were examined. To accomplish this, we created guideline sections corresponding to Chapter 2: Response to an incident after an outbreak and Chapter 3: Collection, acquisition, and maintenance of physical objects in paper media guideline form using GSS-Creator, and then compared observed differences between the GSS and the paper media guideline in terms of the work in that range by objective indicator. This evaluation was based on the time required, and the experiments were performed using the same scenario and criteria that were set for Evaluation 1. The evaluation criteria and results are shown in Table 12.

**Table 12:** Evaluation differences between GSS and the paper media

| Type | Paper media Guideline | GSS |
|---|---|---|
| Time required (Average) | 29 min 41 sec | 24 min 12 sec |

As can be seen in Table 12, when compared with use of the paper media guideline, GSS was evaluated positively regarding the percentage of the time required for the work. Since GSS can properly display the required situation-specific information automatically, we believe it makes a significant contribution because there is no need to look up obscure bits of work information in manuals.

## 9 CONCLUSION

We developed and evaluated an application program named Guideline Total Support System (GSS) that runs on a PC or an Android terminal in order to support implementation of the Guidelines for Preservation of Evidence.
By using an Android terminal to display work contents based on procedures defined in a flowchart, we concluded that it is possible to ensure the work of preserving evidence can be facilitated. Furthermore, we conducted a

comparison of evidence preservation work performed using GSS and paper media using a scenario simulation based on an actual security incident and confirmed the effectiveness of the proposed method.

In the future, after expanding the range of available subject material, it will be necessary to determine whether the GSS is effective in a variety of other incident types. Additionally, because the report generated by GSS-Reporter is expected to be important evidence, we must implement a function to confirm its validity using an electronic signature on an Android terminal at the time the work is carried out. Finally, to increase the number of users, it will be necessary to improve the interface as discussed in the evaluation experiment results.

## 10 REFERENCES


[1] Metropolitan Police Department, Heisei 25 Police White Paper, "Dealing with the threat of cyber space," http://www.npa.go.jp/hakusyo/h25/pdf/pdf/04_tokusyu.pdf

[2] The Institute of Digital Forensics, "About digital forensics," https://digitalforensic.jp/home/what-df/

[3] The Institute of Digital Forensics, Technical workgroup, "The Guidelines for Preservation of Evidence version 3," https://digitalforensic.jp/wp-content/uploads/2014/06/5b0f6b0e93f42b5b3fd27a290d977a681.pdf, September 2013

[4] Ashino, Y., Fujita, K., Furusawa, M., Uehara, T., and Sasaki, R., "Extension and Evaluation of Boot Control for a Digital Forensic System," Advances in Digital Forensics V (Eds. G. Peterson, S. Shenoi), pp. 133-141, 2009.

[5] Kuntze, N., Rudolph, C., Alva, A., and Endicott-Popovsky, B., "On the Creation of Reliable Digital Evidence," Advances in Digital Forensics VIII (Eds. G. Peterson, S. Shenoi), pp. 3-17, 2012.

[6] Osborne, G., Thinyane, H., and Slay, J., "Visualizing Information in Digital Forensics," Advances in Digital Forensics VIII (Eds. G. Peterson, S. Shenoi), pp. 35-47, 2012.

[7] The Information-technology Promotion Agency Japan, "the reconnaissance report of information security phenomenon situation of damage in 2013," p.32 http://www.ipa.go.jp/files/000036465.pdf, January 2014

[8] The Information Security Committee in Education Network, "The occurrences of personal information disclosure of the school and educational facilities in the Heisei 23 fiscal year," http://school-security.jp/pdf/2011_s.pdf

[9] Foundation Center for Educational Computing, "School Information Security Handbook Reference," http://www.cec.or.jp/seculib/handbook/gjskai.pdf, March 2007

[10] The Information-technology Promotion Agency Japan, "the reconnaissance report of information security phenomenon situation of damage in 2013," p.41 http://www.ipa.go.jp/files/000036465.pdf , January 2014

[11] Takahashi, W., Sasaki, R., and Uehara, T., "Development and Evaluation of Guideline Total Support System for Evidence Preservation by Using an Android Phone", CFSE2013 held in Conjunction with COMPSAC2013 (in Kyoto)

[12] Takahashi, W., Sasaki, R., and Uehara, T., "Development of an Application Program to Help Evidence Preservation by Using an Android Phone," 3rd International Conference on e-Education, e-Business, e-Management and e-Learning, pp. 144-149, 2012.

[13] " Cacoo (web application sharing diagram)," https://cacoo.com/

[14] Raghav, S. and Saxena, A.K. Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition, Proceeding of 2009 IEEE Student Conference on Research and Development, pp. 5-8, 2009.

[15] The International Association of Computer Investigative Specialists, "COMPUTER FORENSIC EXAMINER – QUICK REFERENCE GUIDE"

[16] The Japan Network Security Association, "Survey Report about information security incidents in 2011," http://www.jnsa.org/result/incident/data/2011incident_survey_ver14.pdf, December 2012

[17] The Information Security Forum, "Research of the example corresponding to information security accident - in schools, collection of cases," http://www.isef.or.jp/rd/jirei.pdf, April 2014